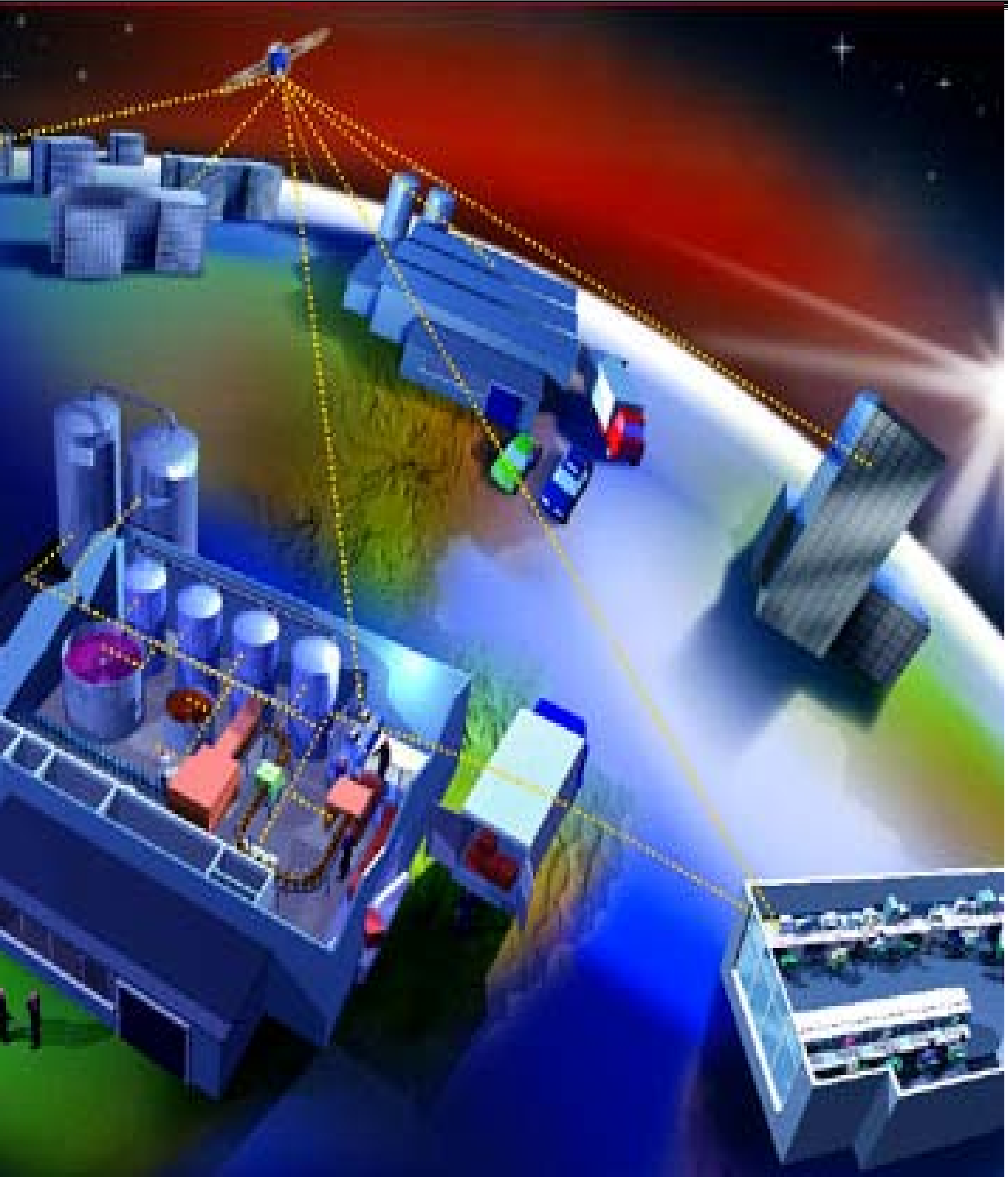


Plant Floor Security

Proposed Agenda for Sector Workshop

Rockwell Automation

Global Manufacturing Solutions

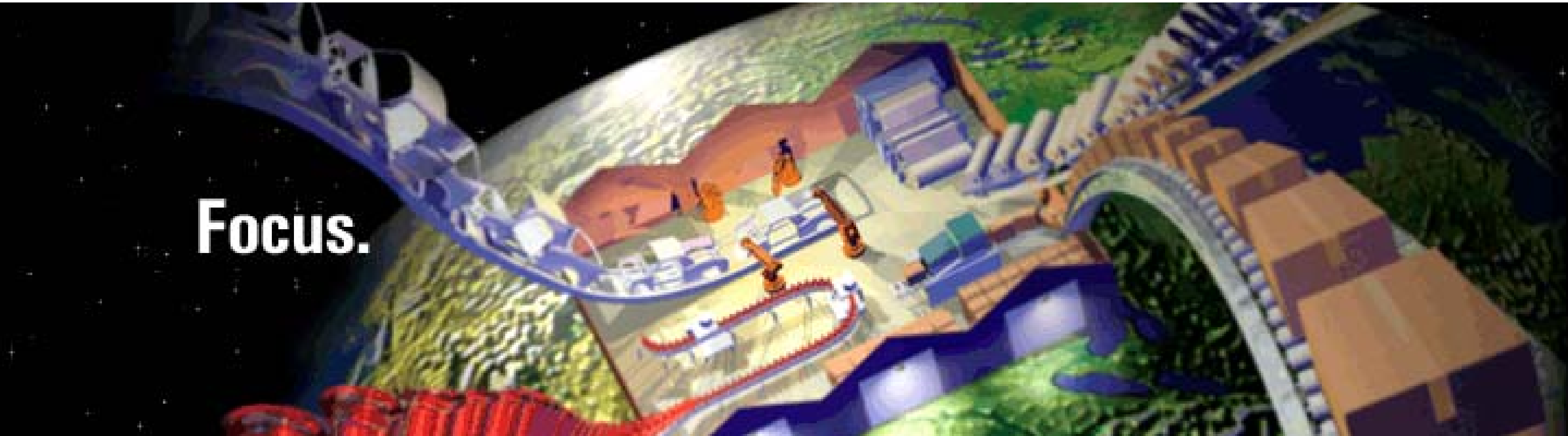
Rockwell Automation

A leading global provider of industrial automation power, control and information solutions that help customers meet their manufacturing productivity objectives:

Reduce costs

Streamline productivity

Speed time to market



At A Glance

- Rockwell acquired Allen-Bradley in 1985, Rockwell Software (ICOM), Reliance Electric and Dodge in 1995
- As of July, 2001 Rockwell operating under the Rockwell Automation name.
- HQ:
  Milwaukee, WI, USA
- FY 2001 Sales:
  $4.3 Billion
- 23,000 employees
- +450 sales
  and support locations
  in +80 countries

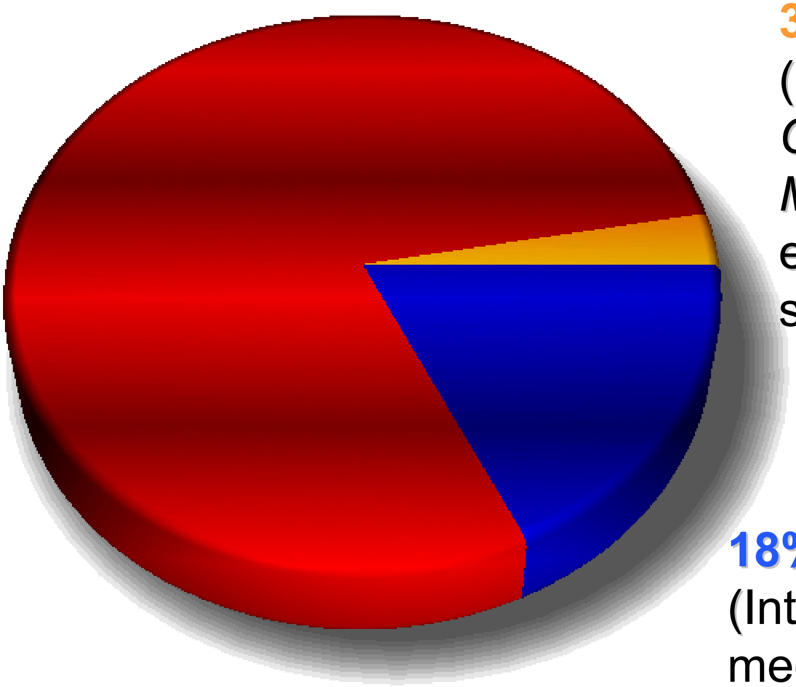
Business Organization

79% - Control Systems (Solutions for integrated sequential, motion, drive system, process and information applications)

Allen-Bradley

ROCKWELL SOFTWARE

Rockwell Automation
Global Manufacturing Solutions



3% - FirstPoint Contact (Solutions that integrate *Customer Relationship Management* with enterprise-wide info systems)

18% - Power Systems (Integrated motor and mechanical power transmission solutions)

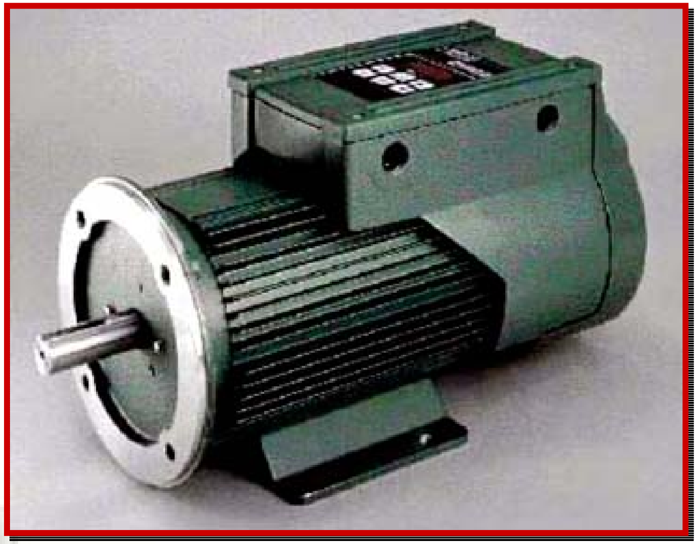
RELIANCE ELECTRIC DODGE

- **Co-own Rockwell Scientific Company with Rockwell Collins**

Reliance Electric Motors And Drives

- Largest industrial motor manufacturer in North America
- Modified and custom motors
- Leader in superconducting motor research
- More than 1 million motor types, styles and sizes
- AC and DC drives

RELIANCE ELECTRIC



DODGE Power Transmission Products

- North America’s No. 1 brand of mechanical power transmission products
- High quality, long-lasting, feature-rich
- One of the most complete lines of mounted bearings, gear reducers and Power Transmission (PT) components
- Innovative, custom product solutions

Mounted Bearings

Gear Reducers

PT & Conveyor Components

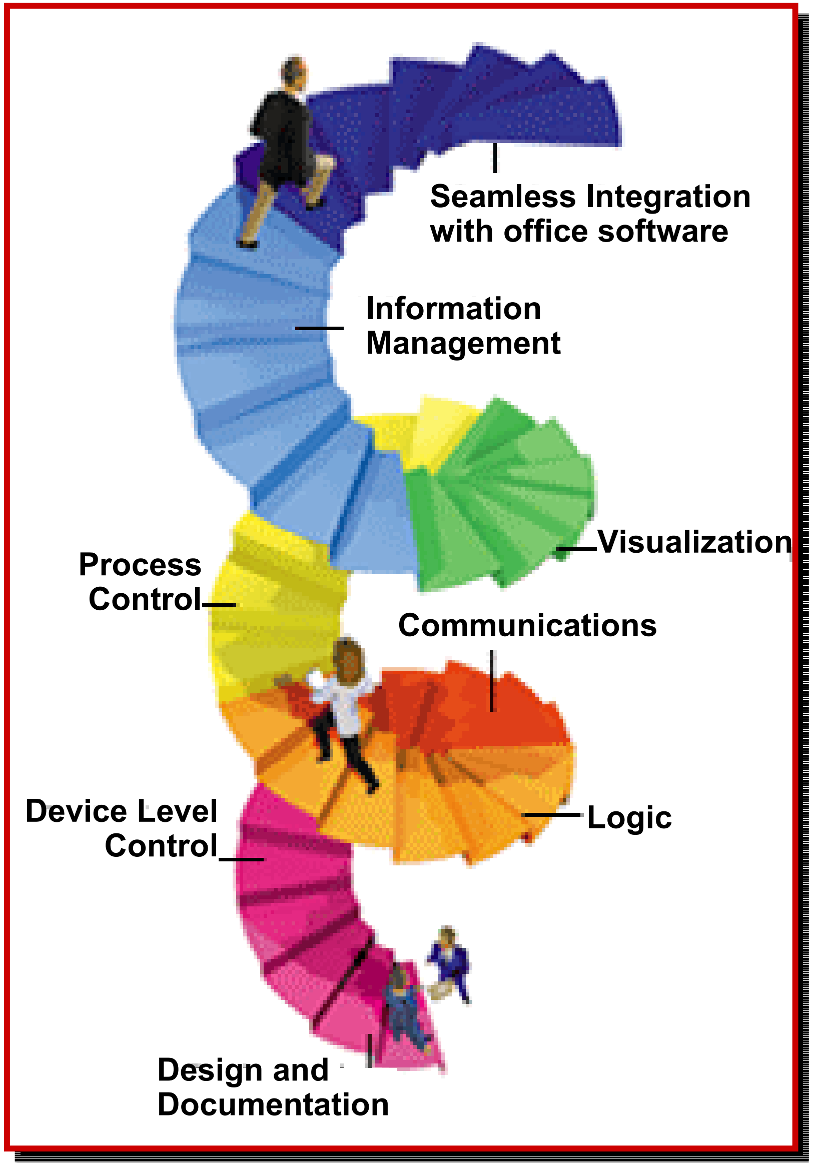
Allen-Bradley Industrial Control Products

- Controllers
- Drives / Motors
- Electronic operator interface devices
- Engineered Solutions
- I/O Systems
- Industrial Computers
- Industrial Controls
- Medium Voltage
- Motion Control
- Motor Control Centers
- Networks & Communication Products
- Open Systems
- Power & Energy Management
- Power Products
- Process Solutions
- Safety
- Sensors
- Software

Rockwell Software Products

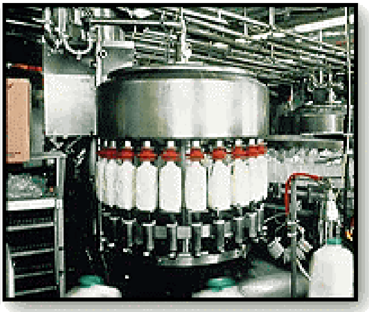
- Mechanical Design
  RSWire
- Communications
  RSLinx, **RS**NetWorx
- Programming software
  RSLogix, **RS**Guardian
- Process Monitoring & Control
  RSBatch, ProcessPak
- Human Machine Interface(HMI) /Visualization
  RSView32
- Information Management
  RSSQL, **RS**Bizware

ROCKWELL SOFTWARE



Industries We Serve

Automotive

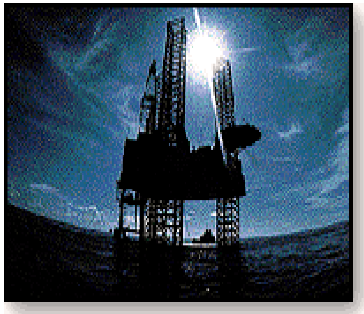


Consumer:
Food, Beverage
& Packaging

Forest Products

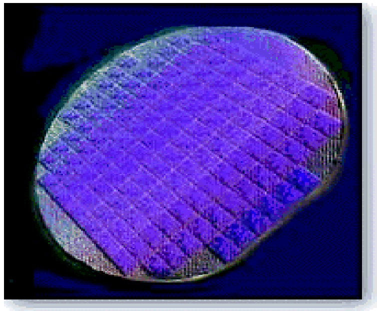
Metals

Mining
& Cement



Petroleum
& Chemical

Pharmaceutical
& Healthcare



Semiconductor

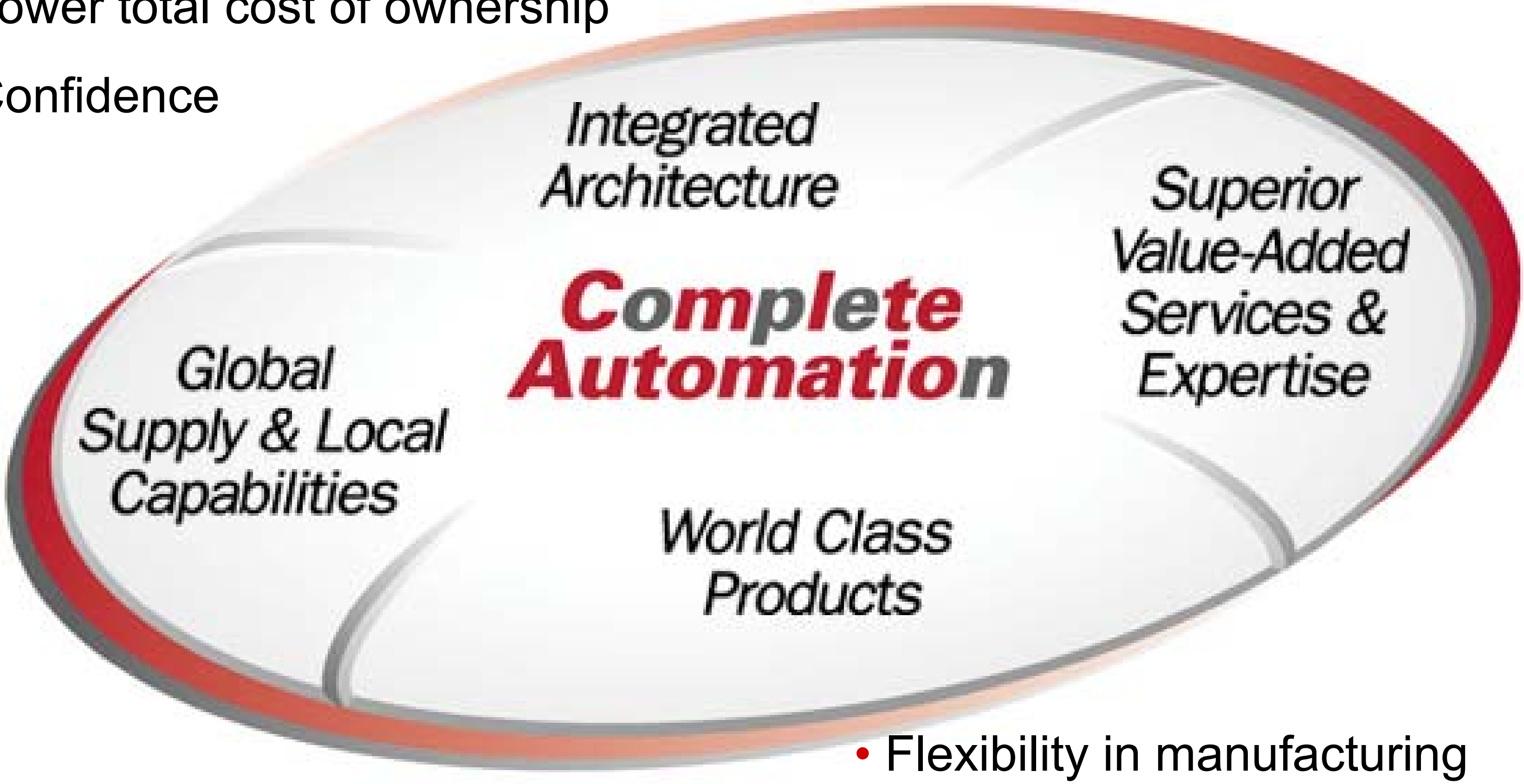
Other Markets

Entertainment
Fiber & Textile
Electric Power
Logistics
Plastics
Airport/Seaport
Waste/Water

🟨 PCSRF target industries

Complete Automation: Meeting Customer Needs

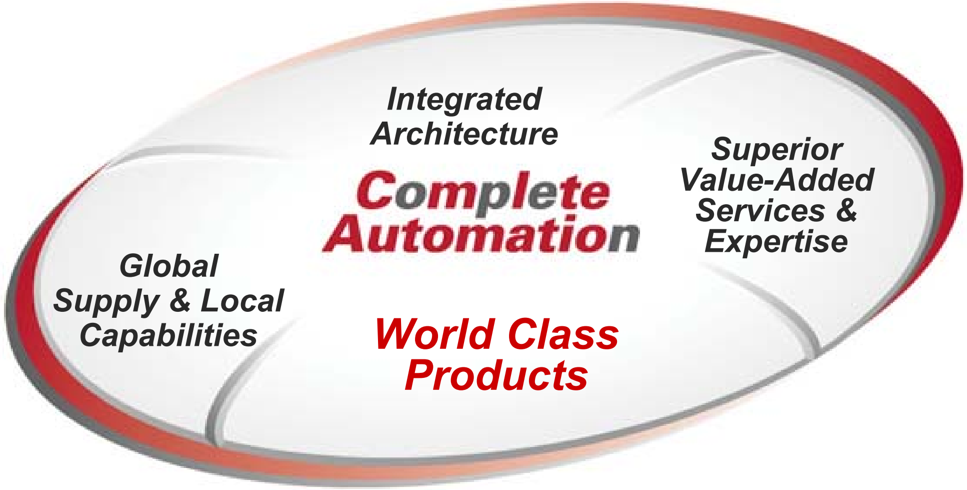
- Lower total cost of ownership
- Confidence


Integrated Architecture
Superior Value-Added Services & Expertise
Complete Automation
Global Supply & Local Capabilities
World Class Products

- Flexibility in manufacturing process
- Greater productivity with fewer resources

World Class Products

- Superior reliability
- Product breadth
- Industry/application-driven design
- Backward compatibility and forward migration
- OPEN technology
- The Best Value



Integrated Architecture

Complete Automation

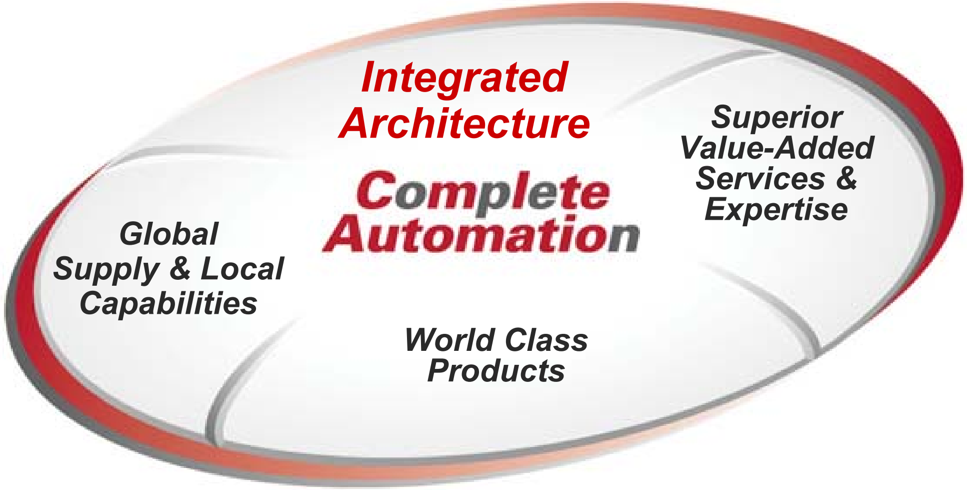
Superior Value-Added Services & Expertise

Global Supply & Local Capabilities

World Class Products

Integrated Architecture

- Choice of technologies
- Industry/application-driven design
- OPEN technology
- Real time control, communication and visualization
- Integrated control and information
- Backward compatibility and forward migration


Integrated Architecture
Complete Automation
Global Supply & Local Capabilities
Superior Value-Added Services & Expertise
World Class Products

World Class Products Connect To Our Integrated Architecture

- Unites products across, and up and down the entire automation system
- By using the same underlying open technologies and a single operating system, products can work, talk and look alike

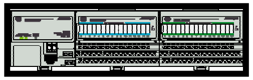
Logix

Controls the process

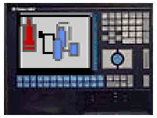
ControlLogix™

ProcessLogix™

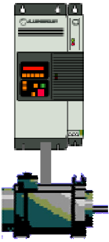
FlexLogix™



SoftLogix™



DriveLogix™



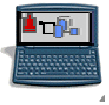
NetLinx

Communicates information across networks

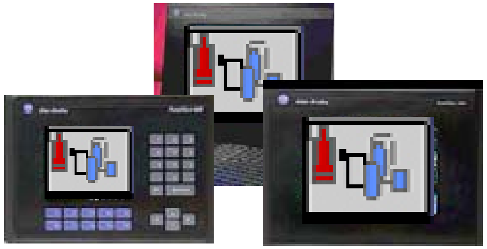
DeviceNet **ControlNet** **EtherNet/IP**

ViewAnyWhere

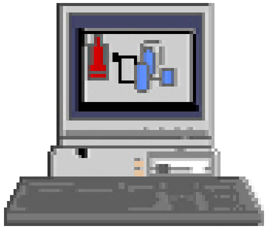
Common framework to **visualize** the process throughout the enterprise system



Pocket HMI



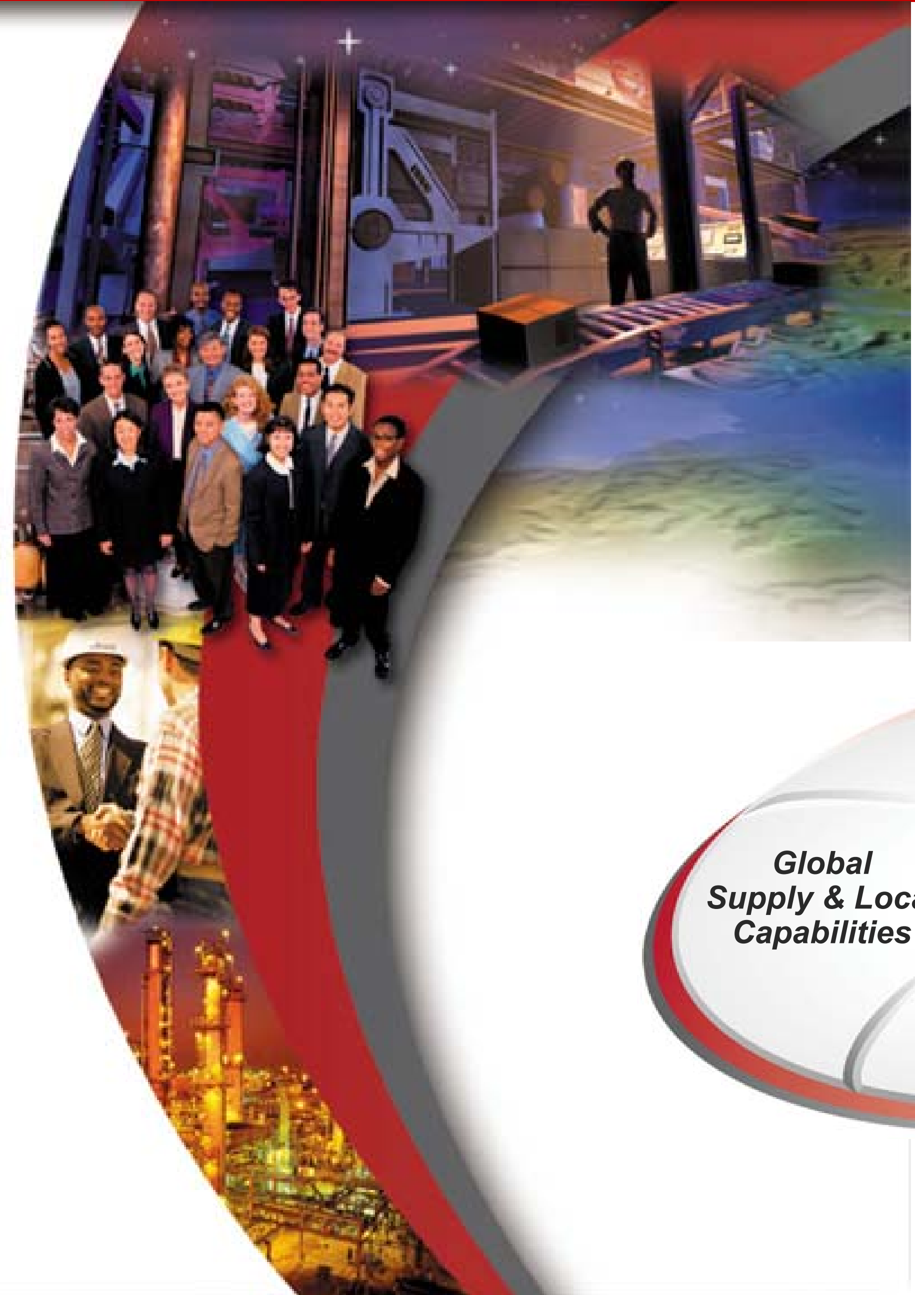
Machine Level HMI



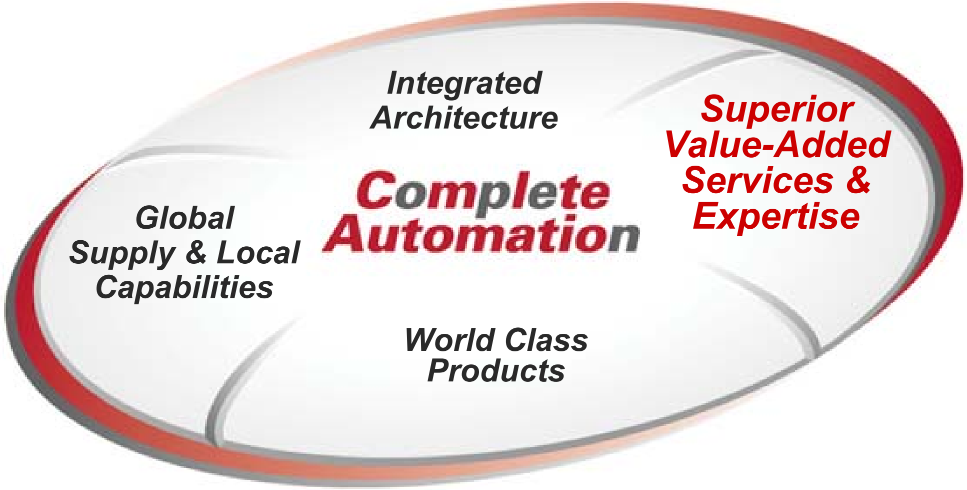
Supervisory HMI

Distributed HMI

Superior Value Added Services & Expertise



- Knowledgeable people
- Long term support
- Responsiveness/immediacy
- OPEN commercial strategy
- Single point of responsibility



Integrated Architecture
Superior Value-Added Services & Expertise
Complete Automation
Global Supply & Local Capabilities
World Class Products

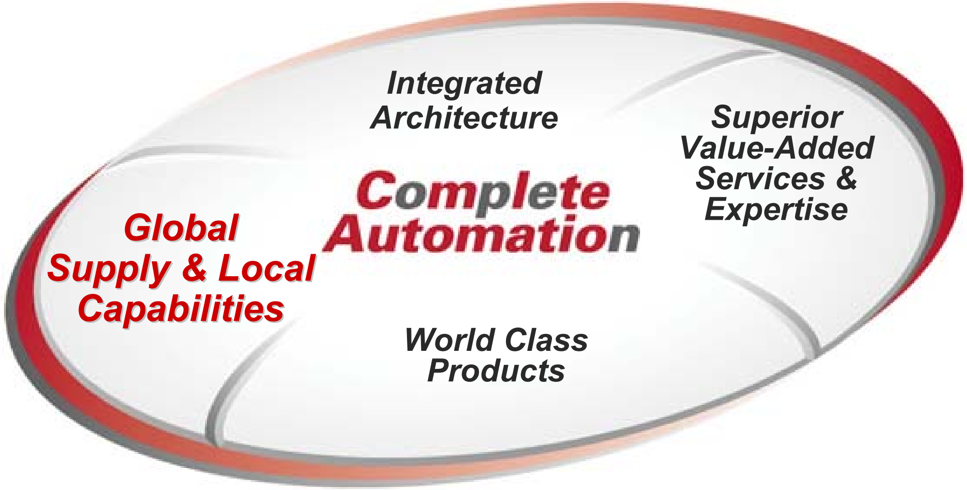
Global Manufacturing Solutions

Helping to make manufacturers more competitive

- Asset Management
- Consulting
- Customer Support
- Engineering Solutions
- Process Solutions
- Training

Global Supply & Local Capabilities

- Worldwide presence
- World-class partnerships
- Reliable expertise and support
- Local, real time availability



Integrated Architecture

Superior Value-Added Services & Expertise

Complete Automation

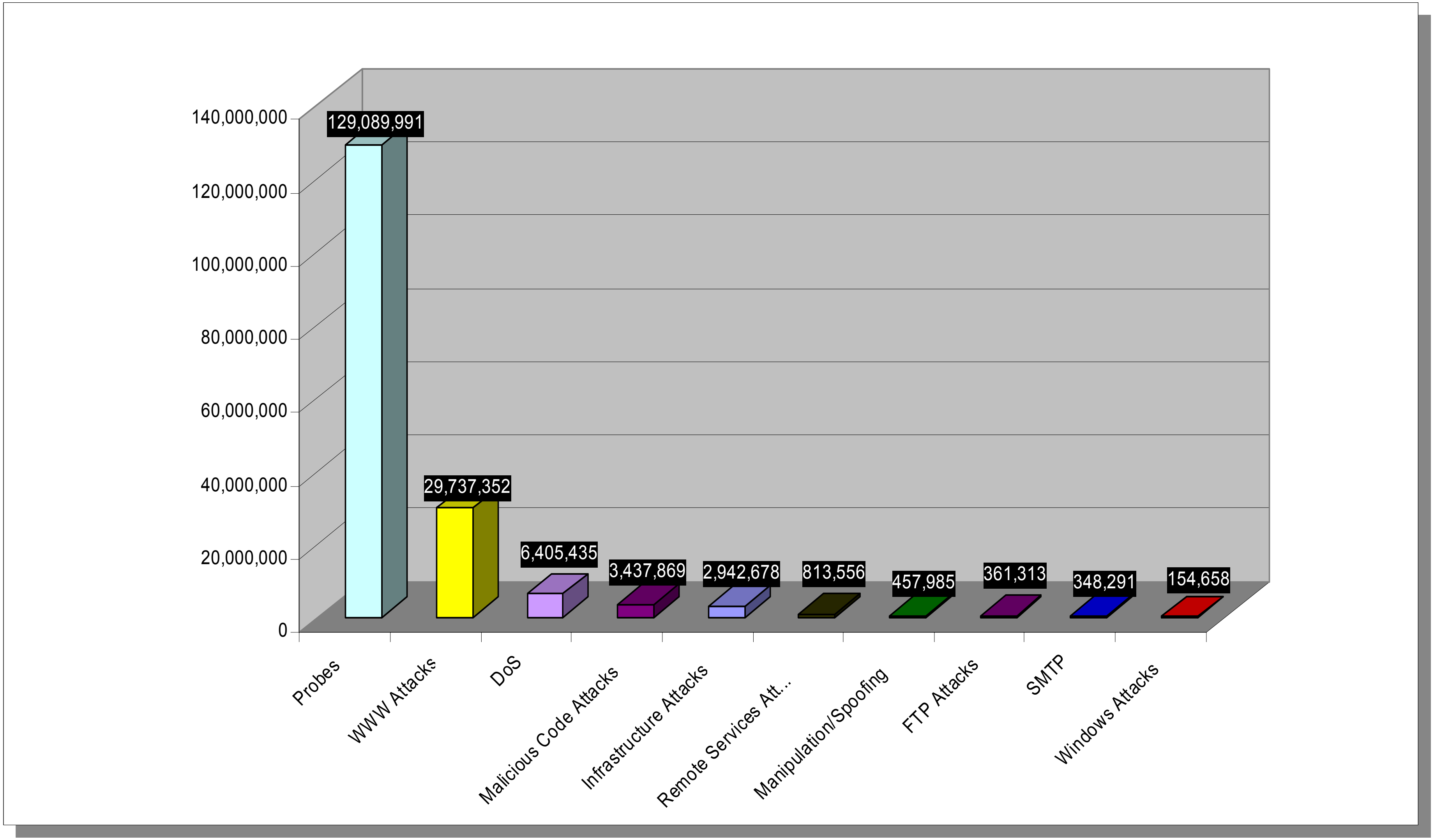
Global Supply & Local Capabilities

World Class Products

Workshop Agenda Ideas

- **Critical manufacturing infrastructure**
  - **Threat scenarios**
  - **Industry concerns**
- Security requirements
- Best practices
- Migration to best practices

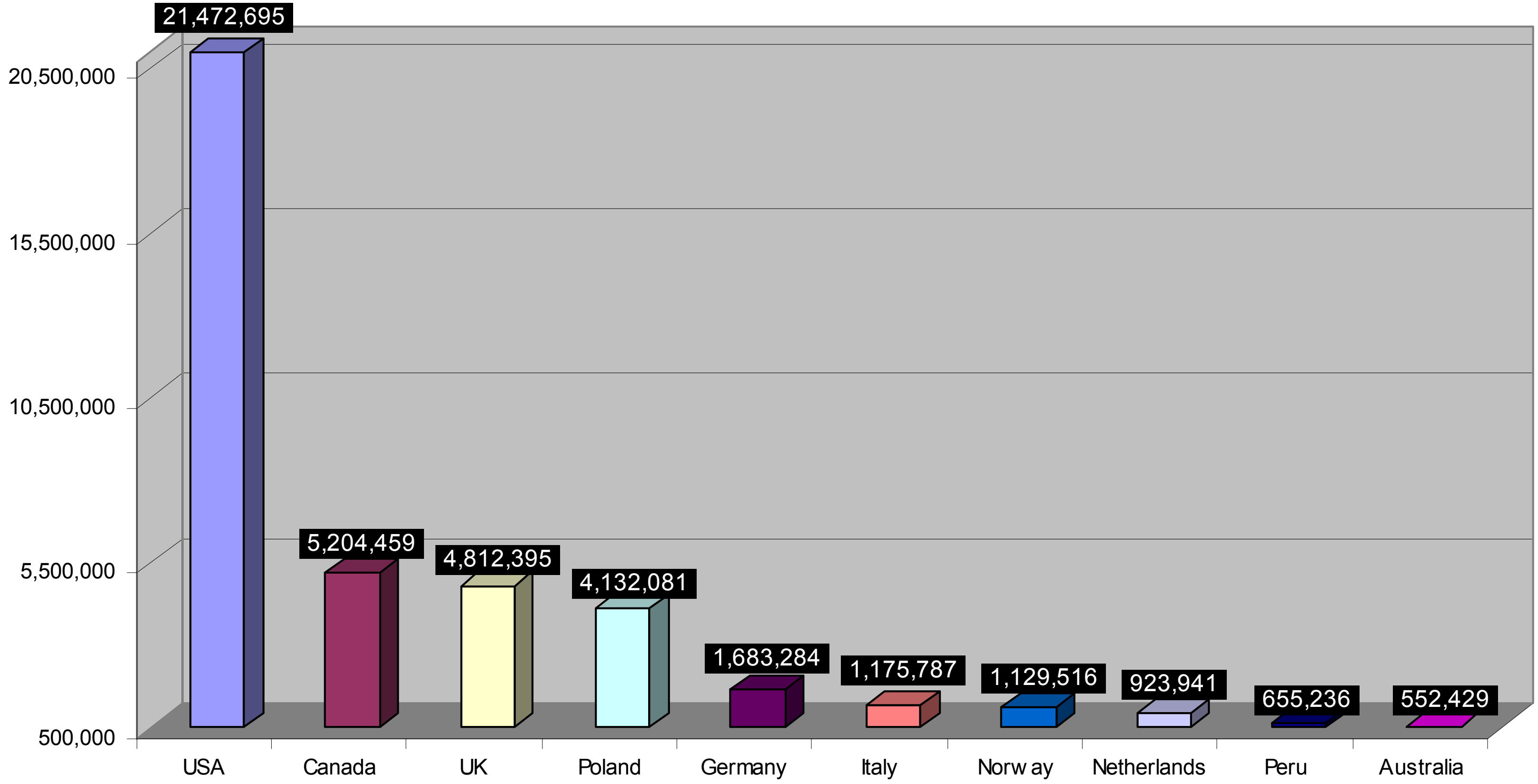
Top 10 Attack Types 2001



Source: Security Focus

Top 10 Attacked Countries 2001

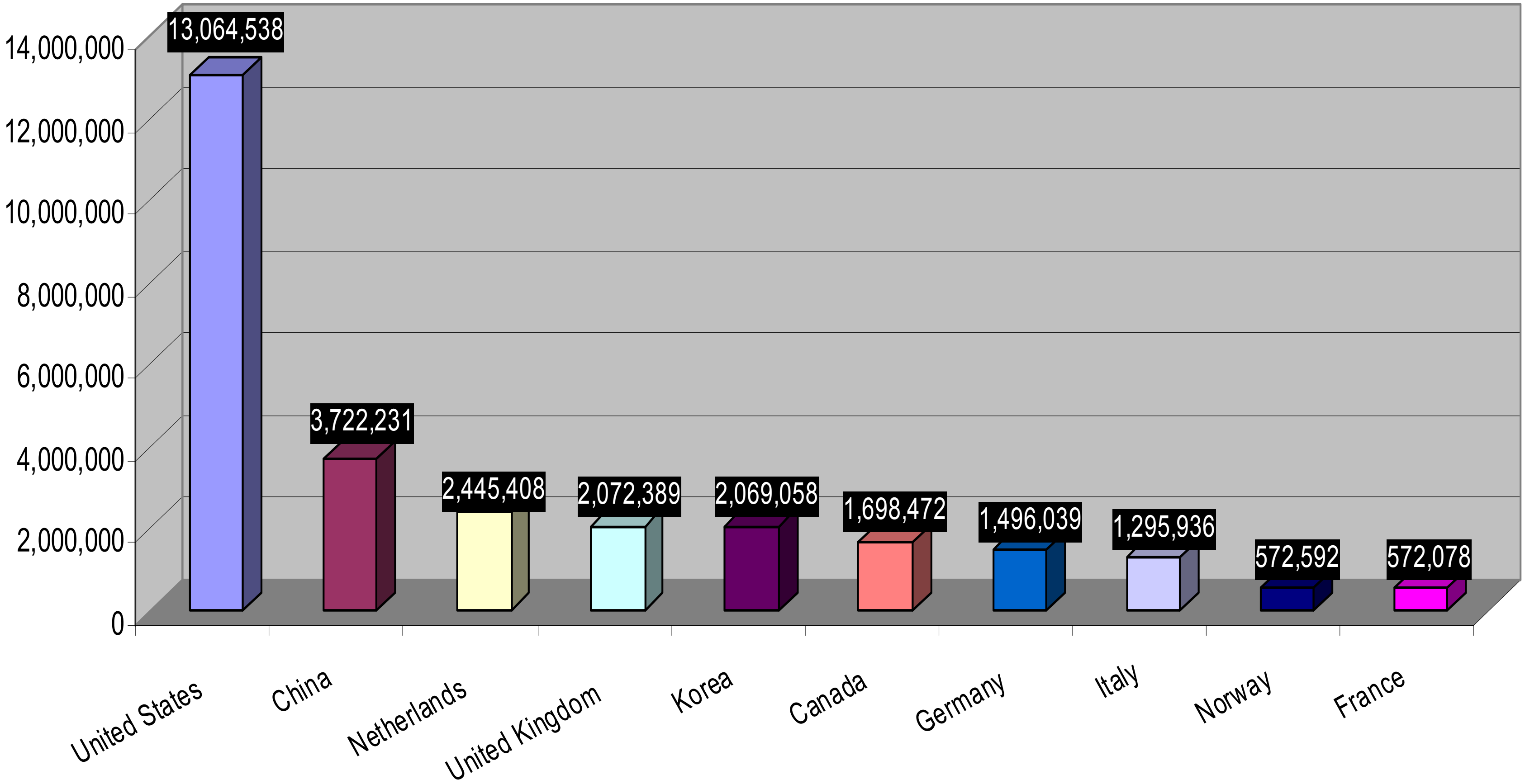
U.S. Attacked More Often Than The Next 9 Countries Combined.



Source: Security Focus

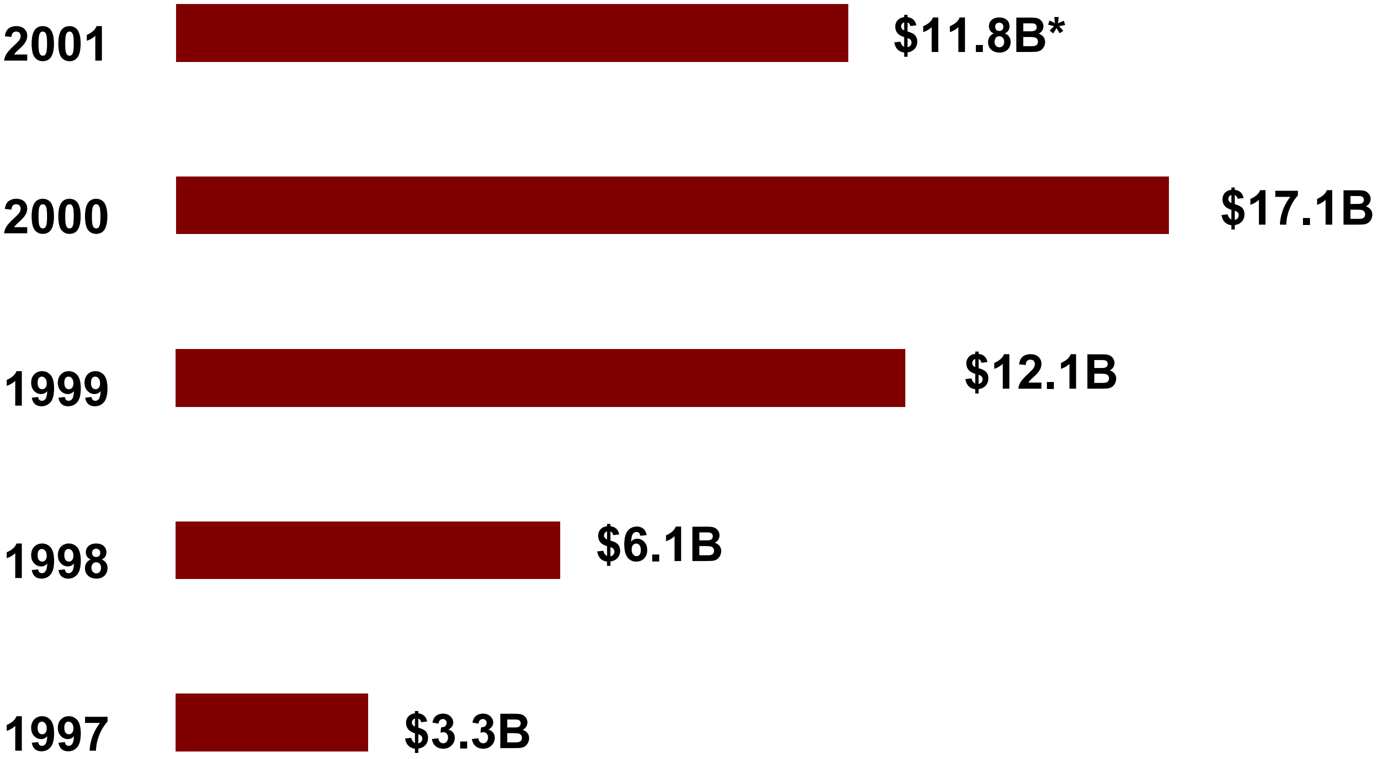
Top 10 Attacking Countries 2001

U.S. Originates Nearly As Many Attacks As The Next 9 Countries Combined.



Source: Security Focus

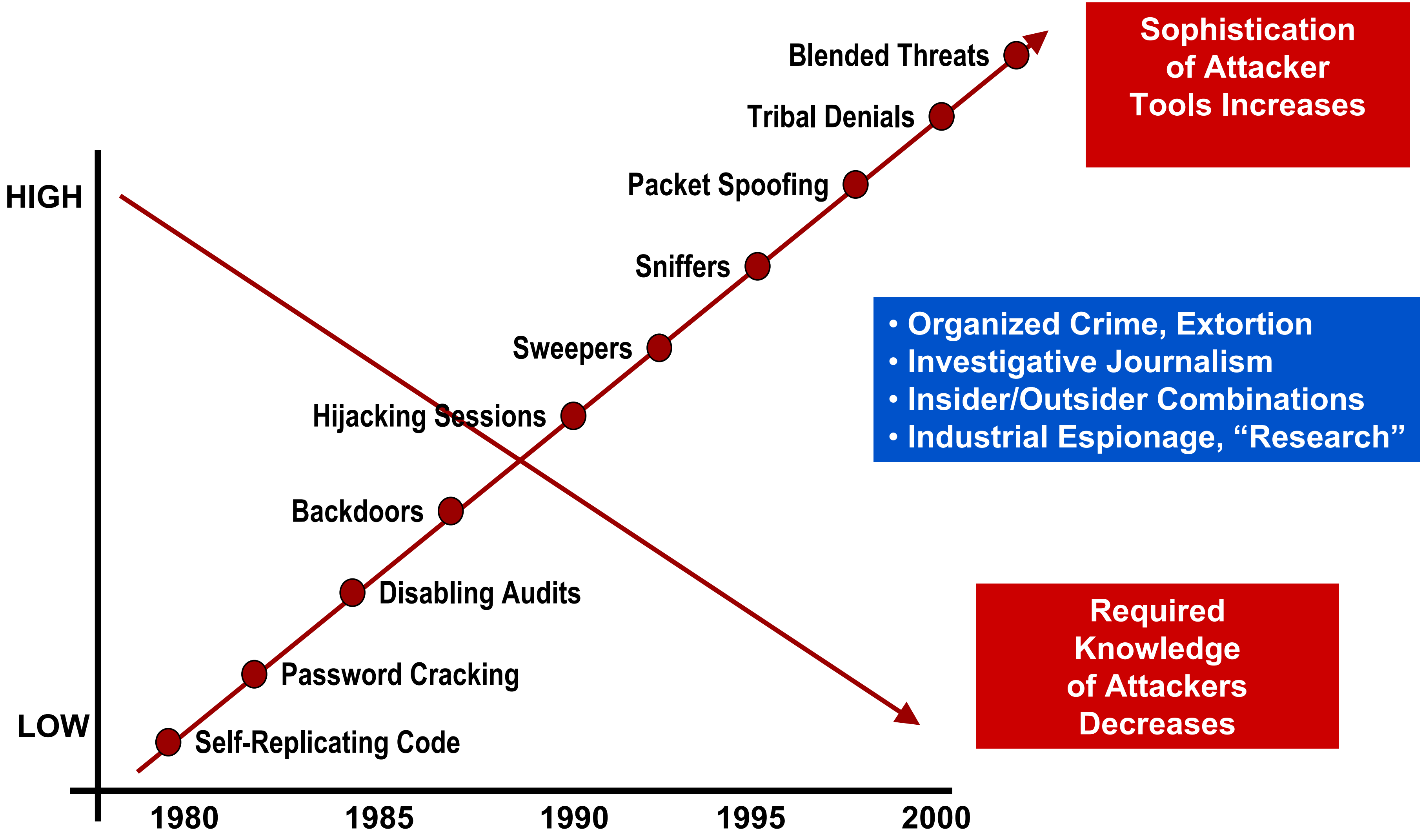
Corporate Losses From Malicious Code Attacks Worldwide



*Through Sept. 22

Source: Computer Economics

Threats Are Real…And Increasing



Sophistication of Attacker Tools Increases

- Organized Crime, Extortion
- Investigative Journalism
- Insider/Outsider Combinations
- Industrial Espionage, “Research”

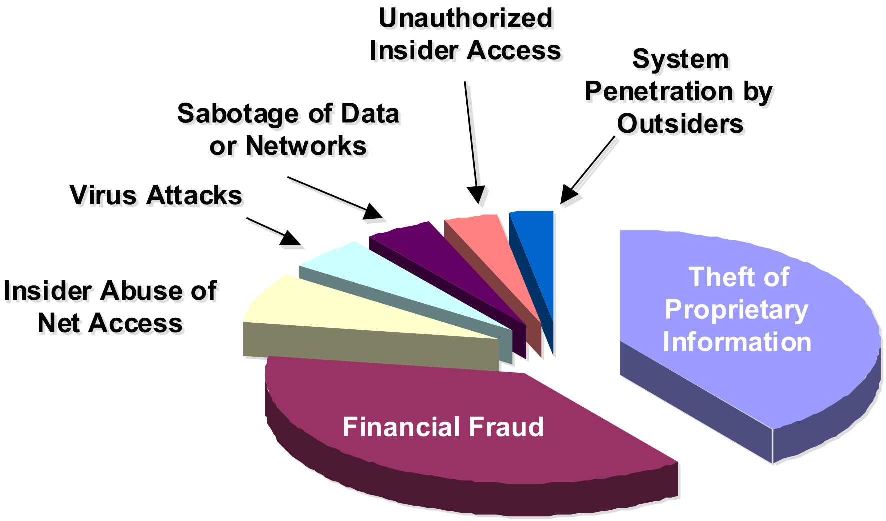
Required Knowledge of Attackers Decreases

2001 FBI Survey Results

521 Business Respondents

Only 161 businesses (31%) could quantify losses

Majority of losses (93%) were attributed to insiders



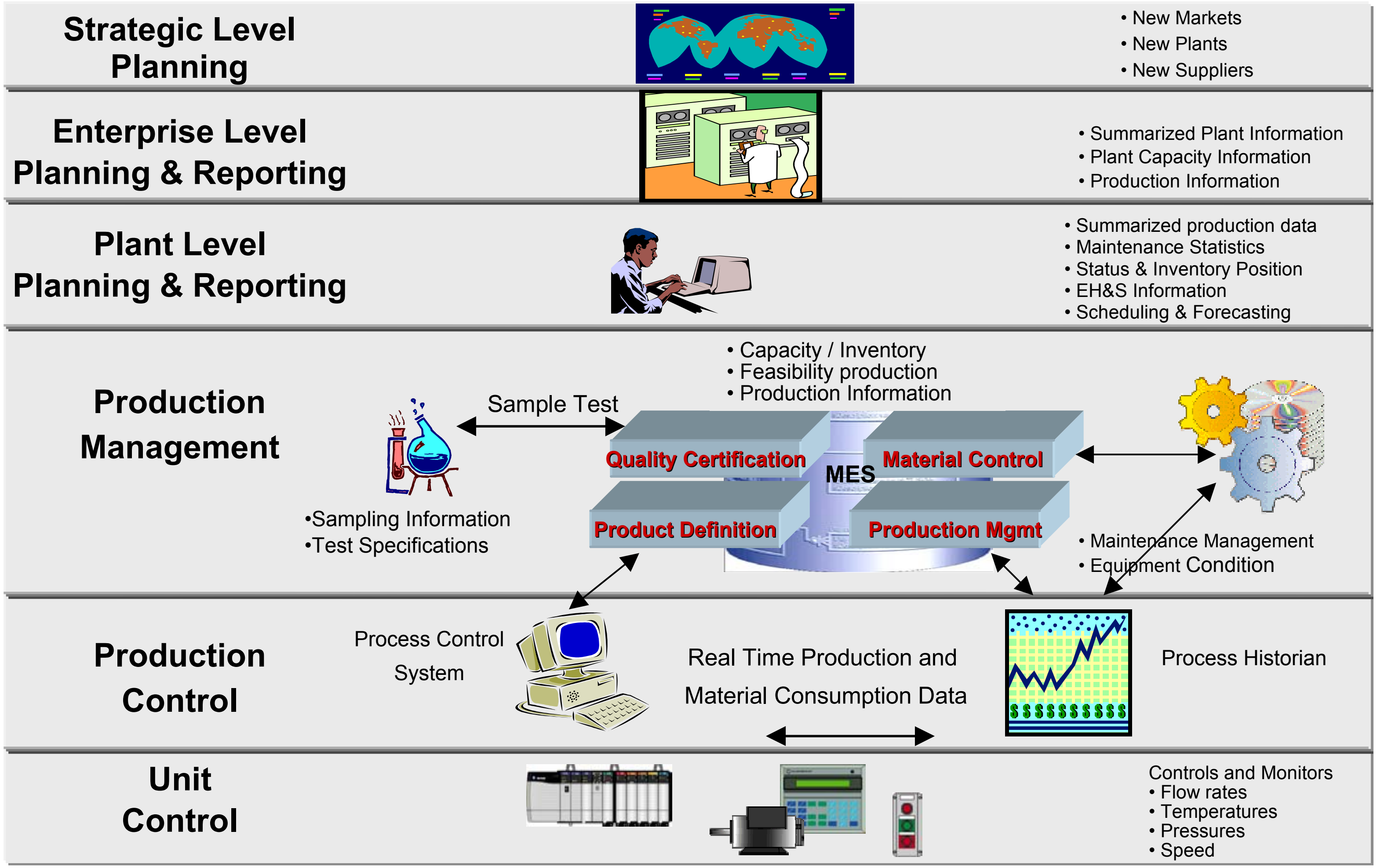
Type of Intrusion	$ Losses
----------------------------	----------------
Information Theft 40%	42,496,000
Financial fraud 37%	39,706,000
Abuse of net access 7%	7,576,000
Virus attacks 5%	5,274,000
Sabotage 4%	4,421,000
Insider misuse 3%	3,567,000
Outsider Penetration 3%	2,885,000
----------------------------	----------------
Total	$105,925,000

Source: “1999 CSI/FBI Computer Crime and Security Survey” Computer Security Institute - www.gocsi.com/losses.htm

Workshop Agenda Ideas

- Critical manufacturing infrastructure
  - Threat scenarios
  - Industry concerns
- **Security requirements**
  - **Plant Floor Protection Profiles**
- Best practices
- Migration to best practices

Business Integration is More Complicated with Security Considerations



Strategic Level Planning

- New Markets
- New Plants
- New Suppliers

Enterprise Level Planning & Reporting

- Summarized Plant Information
- Plant Capacity Information
- Production Information

Plant Level Planning & Reporting

- Summarized production data
- Maintenance Statistics
- Status & Inventory Position
- EH&S Information
- Scheduling & Forecasting

Production Management

- Capacity / Inventory
- Feasibility production
- Production Information

Sample Test

•Sampling Information
•Test Specifications

MES

Quality Certification

Material Control

Product Definition

Production Mgmt

- Maintenance Management
- Equipment Condition

Production Control

Process Control System

Real Time Production and Material Consumption Data

Process Historian

Unit Control

Controls and Monitors
- Flow rates
- Temperatures
- Pressures
- Speed

What Are We Trying To Protect ?

- Confidentiality
- Integrity
- Availability

Production Schedules

Production Rates, C eld

Customer Inf

Proce ns, Setpoints

pecifications, Recipes

perating Procedures

Quality Data

Manufacturing Know-how

What Are We Trying To Protect ?

- Confidentiality
- Integrity
- Availability

Manufacturing Process

Production Equipm

Manufacturi es

Raw nventory

Product Inventory

ersonnel Safety

Environmental Protection

Manufacturing Assets

How Does All Of That Relate To My Plant Floor?

Don't wait for security threats to identify themselves.

Know thy enemy, no matter how cute.

Asking Security Related Questions

What if –

- Your manufacturing systems were hacked and shut down for 22 hours?
- Your production recipes were stolen?
- Your production output was obtained by a competitor?
- A worker was injured?
- A environmental release occurred?
- A process vessel/equipment was damaged?

Security Breaches On The Plant Floor

Real Manufacturing Examples:

- Work Cell Shut Down, Because Of Denial Of Service Attack On A PLC
- New Recipe Downloaded To The Wrong Plant Due To Wrong IP Addressing
- Password Change Of All PLC’s During Labor Dispute
- IT Department Send ICMP Redirect To Test Ethernet Nodes – Plant Shut Down For Two Days
- IT Employee Introduced Virus Into LAN after Lay-off - Plant Shut Down For Two Days

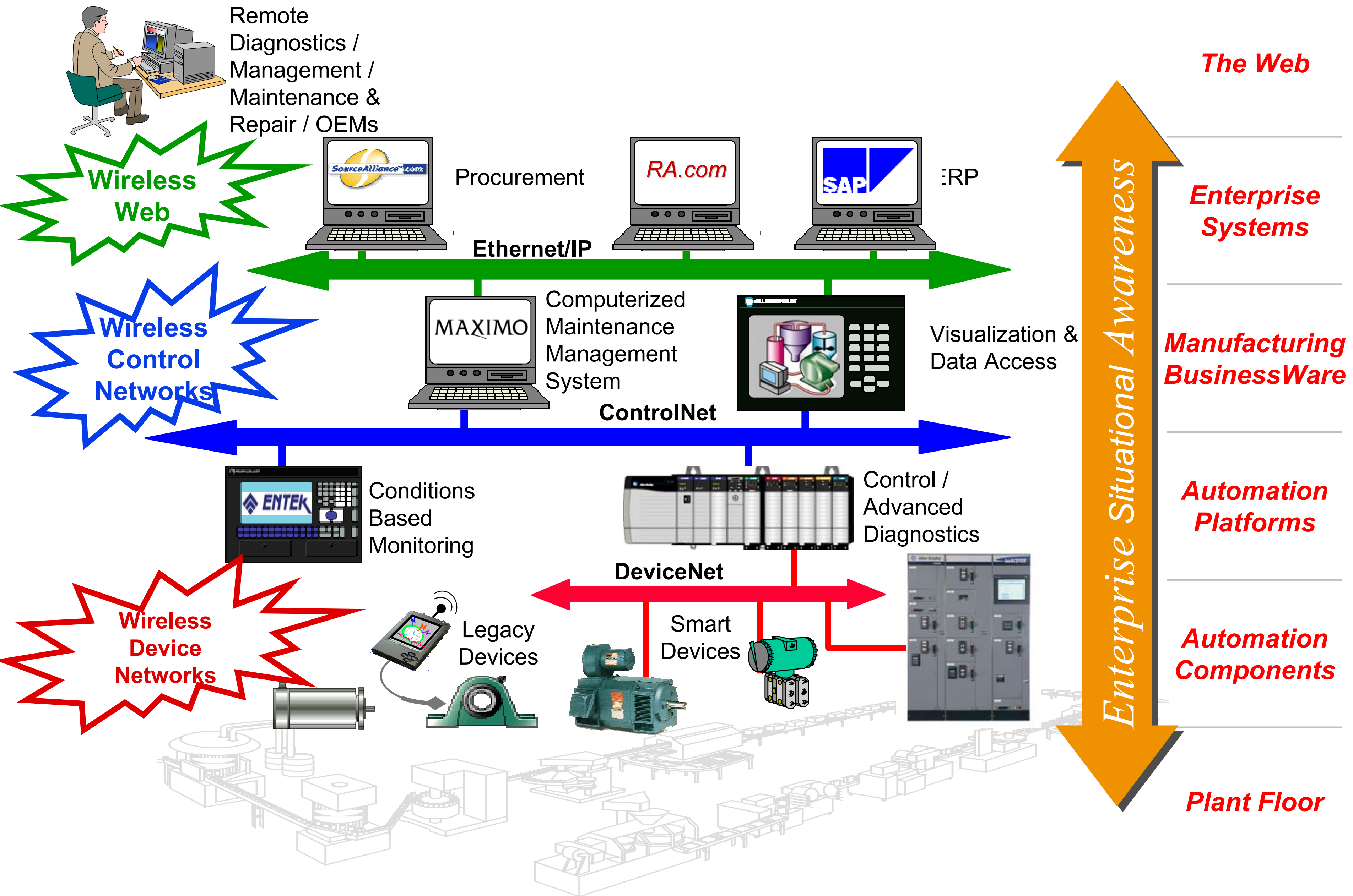
Contents of a Protection Profile

- Introduction
- TOE description
- Security environment
- Security objectives
- Security requirements
- Application notes
- Rationale

Workshop Agenda Ideas

- Critical manufacturing infrastructure
  - Threat scenarios
  - Industry concerns
- Security requirements
  - Plant Floor Protection Profiles
- **Best practices**
  - **DuPont Network Security Assessment Methodology**
- Migration to best practices

Network Security Environment



Remote Diagnostics / Management / Maintenance & Repair / OEMs

Wireless Web

Procurement

RA.com

ERP

Ethernet/IP

Wireless Control Networks

Computerized Maintenance Management System

Visualization & Data Access

ControlNet

Conditions Based Monitoring

Control / Advanced Diagnostics

DeviceNet

Wireless Device Networks

Legacy Devices

Smart Devices

Enterprise Situational Awareness

The Web

Enterprise Systems

Manufacturing BusinessWare

Automation Platforms

Automation Components

Plant Floor

Why DuPont Network Security Assessment Methodology (DNSAM)?

	Evolution of Technology		
Operating Systems:	Proprietary		Open
Data Communication:	Proprietary		Standard Protocols
Information Flow:	Segmented	→	Integrated
Computing Solutions:	Monolithic		Modular
Architecture:	Closed		Open

- Interoperability with higher level business systems has tremendous advantages, but also has increased risk and exposure to information security breaches.
- DuPont Network Security Methodology
  - Developed by DuPont
  - Executed by Rockwell Automation

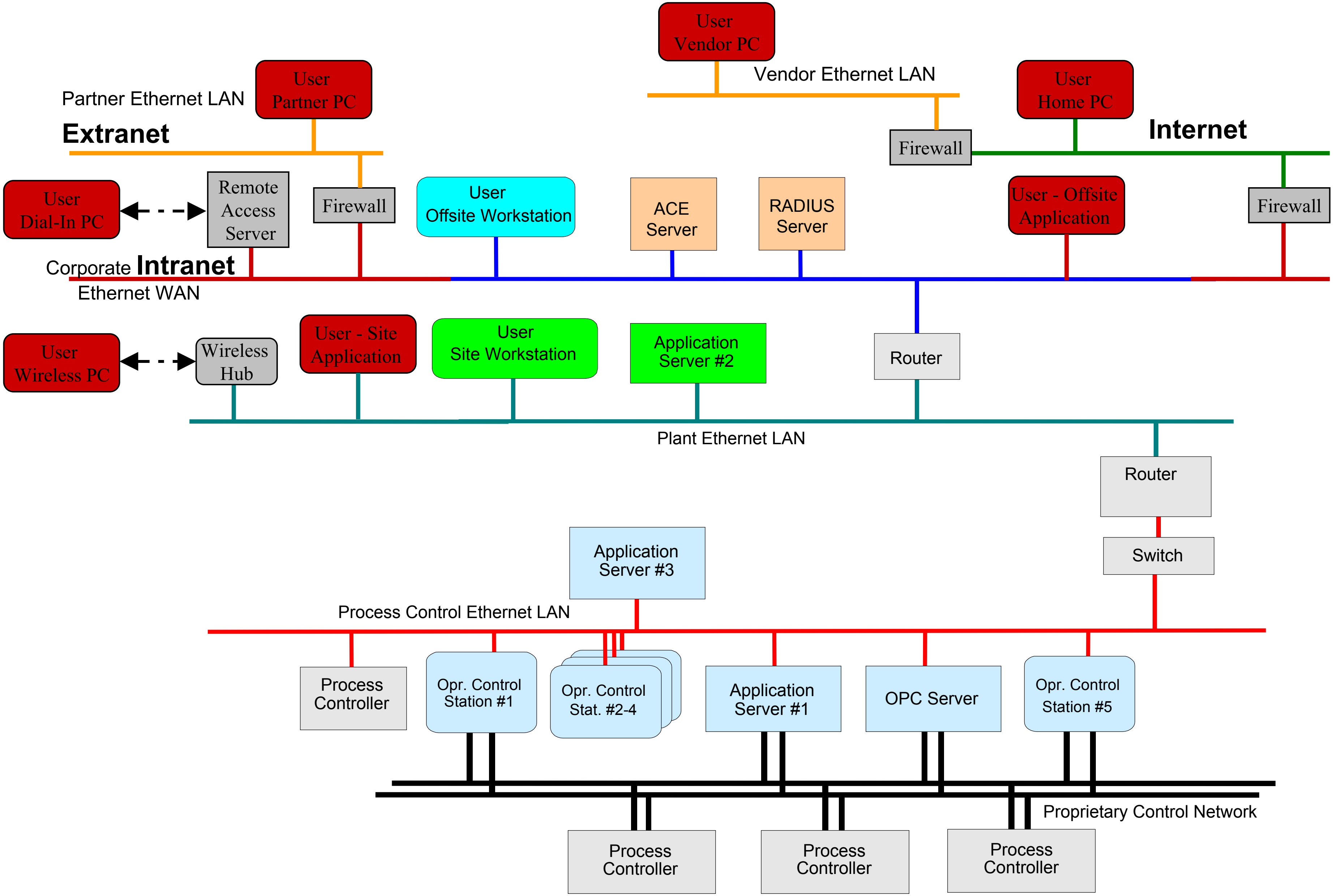
Security Analysis Framework

- Four Steps defined in DNSAM:
  - Review
  - Design
  - Implement
  - Support & Maintain

1st Step - Review

- Review Corporate Information/Security Policies
  - Security requirements
- Solicit Participation From Key Stakeholders
- Understand Functional Objectives
- Understand Threats
  - Provide Education
- Identify Assets To Be Protected
- Analyze Risks

What are the Targets of Evaluation?



Risk Analysis Rating System

Probability	Criticality
A = Very likely	1 = Severe impact
B = Likely	2 = Major impact
C = Not likely	3 = Minor impact
D = Remote chance	4 = No impact

Network Segment	Threat Probability
Internet, Wireless, Direct Dial-in	A = Very likely
Intranet, Secure Dial-in	B = Likely
Integrated PCN	C = Not likely
Isolated PCN	D = Remote Chance

Impact Category	1=Severe impact	2=Major impact	3=Minor impact	4=No impact
Injury	Loss of life or limb	Requiring hospitalization	Cuts, bruises, requiring first aid	None
Financial loss	Millions	$100,000s	$1000s	None
Environmental release	Permanent damage/ Off-site damage	Lasting damage/ On-site damage	Temporary damage/ Local damage	None
Interruption of production	Weeks	Days	Hours	None
Public image	Permanent damage	Lasting blemish	Temporary tarnish	None

Asset Identification & Assessment

Data Assets

The threat is the theft, corruption, or falsification of the following data:	Probability	Criticality
Production schedule	B	3
Production summary data (rates, yields)	B	2
Process variables	B	3
Product quality, raw material and shipment information	A	3
Tuning data/set points	C	4
Product Recipes and Formularies	B	2
Standard operating conditions (SOC)	B	3
Area operating procedures (AOP)		
Historical process data		

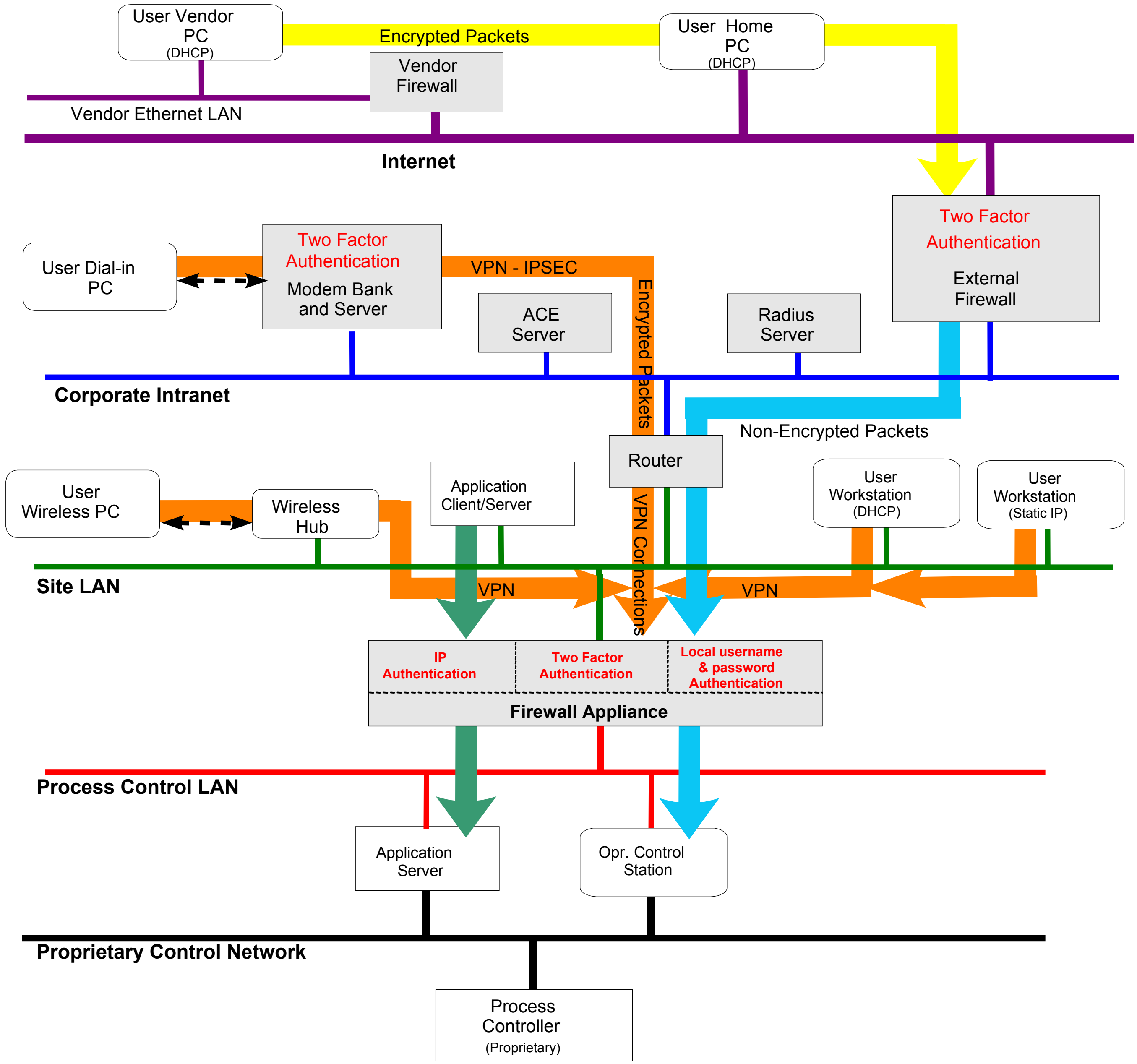
Application & Device Assets

The threat is the corruption, denial of service, or destruction of the following PCN applications/devices:	Probability	Criticality
Operator control station	B	2
Engineering workstation	B	2
PM&C	B	3
Process controller	D	2
External applications gateway	B	3
Control room printer	B	4

2nd Step - Design

- Based on Risk Analysis you select Mitigation Strategies e.g.
  - Placement of Firewalls
  - System Architecture Considerations
  - Strong (two factor) Authentication
  - Digital Certificates
  - Virtual Private Networks / Encryption
  - Policies

3rd Step - Implementation



4th Step - Support & Maintenance

- Site Security Policy Must Address:
  - Access Control
  - Auditing
  - Authorization
  - Disaster Recovery
  - Intrusion Detection
  - Change Management
  - Roles & Responsibilities
  - Vulnerability Analysis

Workshop Agenda Ideas

- Critical manufacturing infrastructure
  - Threat scenarios
  - Industry concerns
- Security requirements
  - Plant Floor Protection Profiles
- Best practices
  - DuPont Network Security Assessment Methodology
- **Migration to best practices**
  - **RA consulting practice**

Proposed Workshop Agenda
Network Security Services

Methodology for deploying secure industrial network solutions for the plant floor

Andreas Somogyi
Practice Leader
Industrial Network Solutions
Global Manufacturing Solutions

GMS - Value Proposition and Vision

Network Security Services Consulting

Global Manufacturing Solutions (GMS)

Rockwell Automation

Value proposition:

To provide solutions and services which enable seamless, high performance and secure data exchange from the plant floor to corporate business systems.

Vision:

To be a preferred global industrial communication network consulting and implementation partner.

GMS- Network Security Services

- **Secure Network Design & Architecture**
  - DuPont Network Security Assessment Methodology
    - Risk Analysis, Application Requirements, Firewall Rule Sets, etc.
- **Network Gateway & Firewall Management Service**
  - Configuration Management
  - Performance, Load Testing
  - Experience: Deployment Of +100 Firewalls Globally
- **VPN's**
  - Remote User VPN's
  - Site to Site/Facility to Facility VPN's
  - Partner/Vendor VPN connections

GMS - Security Services

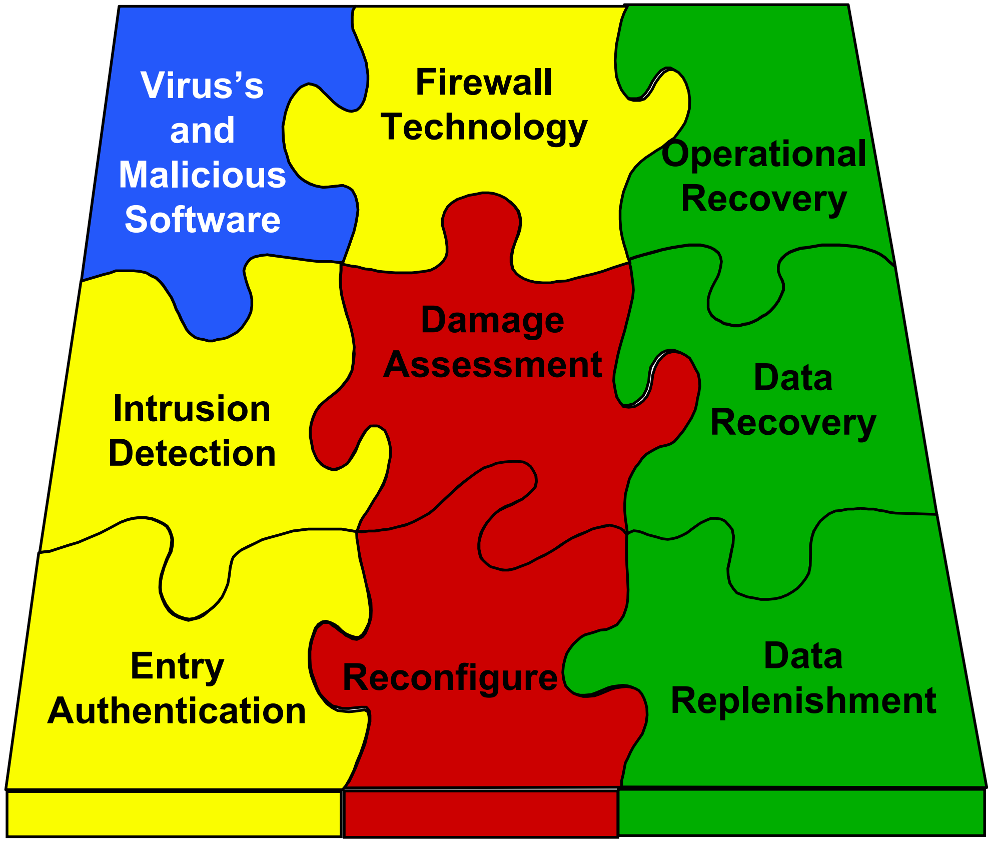
- **Intrusion Detection Services**
  - Requirements Analysis
  - Infrastructure HW/SW Deployment
  - Network-based Intrusion Detection Services (NIDS)
  - Host-based Intrusion Detection Services (HIDS)
  - Configuration Management
    - Version Control, Signature Analysis, Anomaly Detection
  - User Misuse Detection & Assessment

GMS - Security Services

- **Monitoring - 7/24/365 Monitoring Through Network Operation Center**
  - Firewall Services
  - Intrusion Detection Services
  - Critical Business Applications And Assets
  - Performance Monitoring Of VPN's, Firewalls, IDS
  - Web Content Monitoring
  - Host-based Monitoring

Total Security Picture

- A One Time Shoot Doesn't Cut It
- You Need A Complete Interlocked Security Solution, Which Is Tailored To Suit The Unique Needs Of The Organization



🟦 Offensive and malicious component

🟨 Entry denial and regulation

🟥 Diagnosis and beginning recovery

🟩 Operational recovery

Supply Chain Network Solutions - Contacts

Your Contact:

Andreas Somogyi

440 646 3105

Practice Leader

Industrial Network Solutions

asomogyi@ra.rockwell.com

Focused on:

Wireless Solutions, IT-Level Network Integration of Shop Floor to Top Floor, and Network Security Services

OR

Call the Network Service Line
440 646 3030
Discuss Your Opportunity

Thank You for Your Attention

Q&A